UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,599	07/06/2006	Heiko Kober	095309.56901US	6022

23911   7590   09/08/2008
CROWELL & MORING LLP
INTELLECTUAL PROPERTY GROUP
P.O. BOX 14300
WASHINGTON, DC 20044-4300

EXAMINER
ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/553,599	KOBER ET AL.
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _18 October 2005_.
2a) ☐ This action is **FINAL**.   2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _23-44_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _23-44_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _10/18/05_.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1.   This action is in response to the communication filed on October 18, 2005.

Claims 1-22 were originally received for consideration. Per the received preliminary

amendment, claims 1-22 were cancelled and claims 23-44 are added.

2.   Claims 23-44 are currently pending consideration.

Information Disclosure Statement

3.   An initialed and dated copy of Applicant's IDS form 1449, received on

10/18/2005, is attached to this Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 23-44 are rejected under 35 U.S.C. 102(b) as being anticipated by

Thomlinson et al. (U.S. Patent 6,044,155).

Regarding claim 23, Thomlinson discloses:

A method for loading an application program into a program memory of a microprocessor system having a processor bus that is connected to at least one microprocessor; at least one program memory with a boot sector, a flash boot loader, an electrically erasable and programmable memory and a read-write memory; and at least one system interface; said method comprising:

producing an authentication code for the application program (column 9, lines 43-52, column 16, lines 25-67);

reading in the authentication code and the current application program, via the system interface (column 9, lines 43-52, column 16, lines 25-67); and

before a read-in current application program is actuated, checking the authentication code (column 9, lines 43-52, column 16, lines 25-67);

wherein, the authentication code is calculated in a secured area by concatenating the application program with a first secret data string and calculating a hash value from the concatenated application program (column 9, lines 43-52, column 16, lines 25-67);

the hash value is read into the microprocessor system, via the system interface, as an authentication code (column 9, lines 43-52, column 16, lines 25-67);

a second, identical, secret data string is stored in the microprocessor system (column 9, lines 43-52, column 16, lines 25-67);

the read-in application program is concatenated with the second secret data string in the microprocessor system (column 9, lines 43-52, column 16, lines 25-67); and

a hash value is calculated by the read-in, concatenated application program in the microprocessor and is compared with the transmitted authentication code (column 17, lines 1-5).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Thomlinson discloses:

The method as claimed in claim 23, wherein:

the application program is concatenated with the first secret data string in the microprocessor at the start of the program and at the end of the program, both in the secured area and during the authenticity checking (column 12, lines 35-47, column 9, lines 43-52, column 16, lines 25-67);

a hash value is calculated using the application program which is concatenated at both ends (column 9, lines 43-52, column 16, lines 25-67); and

the hash value is read in as an authentication code at the system interface (column 9, lines 43-52, column 16, lines 25-67).

Claim 25 is rejected as applied above in rejecting claim 23. Furthermore, Thomlinson discloses:

The method as claimed in claim 23, wherein:

the application program is initially concatenated with the first secret data string either at the start of the program or at the end of the program (column 9, lines 43-52, column 16, lines 25-67);

in a following step, a first hash value is calculated in the secured area by using

the application program which is concatenated at one end (column 7, lines 54-59,

column 9, lines 43-52, column 16, lines 25-67);

in a subsequent step, the first hash value is concatenated with a first secret data

string at one end (column 9, lines 43-52, column 16, lines 25-67);

in a still further step, a second hash value is calculated by the combination of a

first hash value and the first secret data string, and said second hash value is read in as

an authentication code at the system interface (column 9, lines 43-52, column 16, lines

25-67);

a second, identical, secret data string is stored in the microprocessor system and

the steps carried out in the secured area are repeated with the original application

program in the same sequence using said second secret data string in the

microprocessor (column 9, lines 43-52, column 16, lines 25-67); and

the hash value which is calculated in the microprocessor is compared with the

hash value which is read in at the system interface (column 17, lines 1-5).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Thomlinson

discloses:

The method as claimed in claim 25, wherein the authentication code is

transferred together with the application program (column 9, lines 43-52, column 16,

lines 25-67).

Claim 27 is rejected as applied above in rejecting claim 25. Furthermore, Thomlinson discloses:

The method as claimed in claim 25, wherein the authentication code is transferred separately from the application program (column 9, lines 43-52, column 16, lines 25-67).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Thomlinson discloses:

The method as claimed in claim 27, wherein:

the application program is stored and distributed in a memory medium (column 9, lines 43-52, column 16, lines 25-67); and

the authentication code is transmitted to the system interface from the secured area by means of data transmission (column 9, lines 43-52, column 16, lines 25-67).

Claim 29 is rejected as applied above in rejecting claim 26. Furthermore, Thomlinson discloses:

The method as claimed in claim 26, wherein the application program and the authentication code are transmitted to the system interface from the secured area by data transmission (column 9, lines 43-52, column 16, lines 25-67)

Claim 30 is rejected as applied above in rejecting claim 29. Furthermore, Thomlinson discloses:

The method as claimed in claim 29, wherein the authentication code is read into a control unit of a motor vehicle via the diagnostic interface (column 9, lines 43-52, column 16, lines 25-67).

Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Thomlinson discloses:

The method as claimed in claim 30, wherein if a read-in authentication code and a hash value calculated in the microprocessor correspond, the associated application program is provided with an identifier as a valid application program (column 9, lines 43-52, column 16, lines 25-67).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Thomlinson discloses:

The method as claimed in claim 31, wherein flashware meta information is included in the authentication code (column 9, lines 43-52, column 16, lines 25-67).

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Thomlinson discloses:

The method as claimed in claim 32, wherein the authentication code is used to selectively download the application program into various control units (column 9, lines 43-52, column 16, lines 25-67).

Regarding claim 34, Thomlinson discloses:

A method for safeguarding authenticity of flashware for a control unit of a motor vehicle in which an application program is stored in a program memory; said method comprising:

in a secured area, concatenating the application program with a first secret data string, and calculating a hash value using the concatenated application program (column 12, lines 35-47, column 9, lines 43-52, column 16, lines 25-67);

reading the hash value into the control unit as an authentication code (column 9, lines 43-52, column 16, lines 25-67);

storing a second, identical, secret data string in the control unit (column 9, lines 43-52, column 16, lines 25-67);

concatenating application program with the second secret data string in the control unit (column 9, lines 43-52, column 16, lines 25-67);

calculating a second hash value using the concatenated application program in the control unit (column 9, lines 43-52, column 16, lines 25-67); and

comparing the calculated second hash value with the transmitted authentication code (column 17, lines 1-5).

Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Thomlinson discloses:

The method as claimed in claim 34, wherein:

the application program is concatenated with the first secret data string in the

control unit at the start of the program and at the end of the program, both in the

secured area and during the authentication checking (column 9, lines 43-52, column 16,

lines 25-67);

a hash value is calculated using the application program which is concatenated

at both ends (column 9, lines 43-52, column 16, lines 25-67); and

the hash value is read in as an authentication code at the system interface

(column 9, lines 43-52, column 16, lines 25-67).

Claim 36 is rejected as applied above in rejecting claim 34. Furthermore, Thomlinson

discloses:

The method as claimed in claim 34, wherein:

the application program is initially concatenated with the first secret data string

either at the start of the program or at the end of the program (column 9, lines 43-52,

column 16, lines 25-67);

in a following step, a first hash value is calculated in the secured area using the

application program which is concatenated at one end (column 9, lines 43-52, column

16, lines 25-67);

in a subsequent step, the first hash value is concatenated with a first secret data

string at one end (column 9, lines 43-52, column 16, lines 25-67);

in a still further step, a second hash value is calculated by the combination of a

first hash value and the first secret data string, and said second hash value is read in as

an authentication code at the system interface (column 9, lines 43-52, column 16, lines

25-67);

a second, identical, secret data string is stored in the control unit and the steps

carried out in the secured area are repeated with the original application program in the

same sequence using said data string in the control unit (column 9, lines 43-52, column

16, lines 25-67); and

the hash value which is calculated in the control unit is compared with the hash

value which is read in at the system interface (column 17, lines 1–5).

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Thomlinson

discloses:

The method as claimed in claims 36, wherein the authentication code is

transferred together with the application program (column 9, lines 43-52, column 16,

lines 25-67).

Claim 38 is rejected as applied above in rejecting claim 36. Furthermore, Thomlinson

discloses:

The method as claimed in claim 36, wherein the authentication code is

transferred separately from the application program (column 9, lines 43-52, column 16,

lines 25-67).

Claim 39 is rejected as applied above in rejecting claim 38. Furthermore, Thomlinson discloses:

The method as claimed in claim 38, wherein the application program is stored and distributed in a memory medium (column 9, lines 43-52, column 16, lines 25-67); and

the authentication code is transmitted to the system interface from the secured area by means of data transmission (column 9, lines 43-52, column 16, lines 25-67).

Claim 40 is rejected as applied above in rejecting claim 37. Furthermore, Thomlinson discloses:

The method as claimed in claim 37, wherein the application program and the authentication code are transmitted to the system interface from the secured area by means of data transmission (column 9, lines 43-52, column 16, lines 25-67).

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Thomlinson discloses:

The method as claimed in claim 40, wherein the authentication code is read into a control unit of a motor vehicle via the diagnostic interface (column 9, lines 43-52, column 16, lines 25-67).

Claim 42 is rejected as applied above in rejecting claim 41. Furthermore, Thomlinson discloses:

The method as claimed in claim 41, wherein if a read-in authentication code and a hash value calculated in the control unit correspond, the associated application program is provided with an identifier as a valid application program (column 9, lines 43-52, column 16, lines 25-67).

Claim 43 is rejected as applied above in rejecting claim 42. Furthermore, Thomlinson discloses:

The method as claimed in claim 42, wherein flashware meta information is included in the authentication code (column 9, lines 43-52, column 16, lines 25-67).

Claim 44 is rejected as applied above in rejecting claim 43. Furthermore, Thomlinson discloses:

The method as claimed in claim 43, wherein the authentication code is used to selectively download the application program into various control units (column 9, lines 43-52, column 16, lines 25-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

                                                        /Kaveh Abrishamkar/
                                                        Examiner, Art Unit 2131

/K. A./
09/02/2008
Examiner, Art Unit 2131